UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/991,057	11/21/2001	James D. Lyle	SII-800 [SIMG0103]	3778

7590 01/23/2006

Alfred A. Equitz
GIRARD & EQUITZ LLP
Suite 1110
400 Montgomery Street
San Francisco, CA 94104

EXAMINER	
POLTORAK, PIOTR	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 01/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/991,057	**Applicant(s)** LYLE, JAMES D.	
	Examiner Peter Poltorak	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 October 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36,53-57 and 70-87* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36,53-57 and 70-87* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

1/12/06.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-36, 53-57 and 70-87 have been examined.

Claim Objections

2. Claims 1-3, 9, 11, 14, 16, 27-29, 31, 53, 57 and 75-76 are objected to because the abbreviation "TMDS" as recited in the claims language must be defined, at least once at the first appearance.

3. Similarly applicant should disclose non abbreviate terms of AES and HDCP protocols cited in claims 27-30.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1-36, 53-57 and 70-87 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that applicant regards as the invention.

5. The phrase "TMDS-like communication link" in claims 1-3, 9, 11, 14, 16, 21, 27-29, 31, 40, 53, 57, 63, 75-76 and 87 renders the claims indefinite because the claims include elements not actually disclosed (those encompassed by "TMDS-like communication link"), thereby rendering the scope of the claims unascertainable. See MPEP pg. § 2173.05(d).

6. Also, the applicant should define an abbreviation in the claim language at least when the abbreviation is cited for the first time.

7. The phrase: “the pre-encrypted version of the key” in claim 36 is not understood. Similar language is used in some other claims (1, 12, 15, 17-19, 22-25, 32, 36, 46, 53, 57, 86-87), e.g. claim 1 recites: “an encrypted version of the secret value”. For purposes of further examination the term “version” is treated as though emphasizing action performed to the object of the version, e.g. an encrypted version of the secret value is treated as “an original secret value that is encrypted”.

8. Claim 57 recites:

   “and wherein the external agent is also operable in a second mode in which it sends a control signal to the transmitter and a second control signal to the receiver, wherein the transmitter is configured to operate in a pass-through mode in response to the control signal and the receiver is configured to operate

   in a non-decrypting mode in response to the second control signal, wherein, in the pass-through mode, the transmitter receives data from a source and transmits the data over the at least one TMDS-like link to the receiver without encrypting said data,

   and in the non-decrypting mode, the receiver does not decrypt the data that it receives from the transmitter over the at least one TMDS-like link”.

9. The claim language is ambiguous. It is not clear how particular limitations relate to each other. For example, it is not clear whether the claim language suggests that the transmitter receives data from a source and transmits the data over a link to the

receiver and that this receiving is called a pass-through mode or whether the transmitter would have the ability to operate in such a mode *("operable" is not a positive recitation requiring only that a subject has the capability to operate in a particular fashion and not that this activity actually occurs)* in which the transmitter could receive data from a source and transmit the data to the receiver.

Furthermore it is not clear whether "pass-decrypting mode" is a condition that occurs during the transmitter operating in the "second mode", or whether the non-decrypting mode simply further limits the operations of the receiver without any link between the "pass-through" and the "non-decrypting" modes.

For purposes of further examination the phrase is treated as best understood.

10. The phrase: "wherein the switch is coupled ... 'to assert the encrypted data over a selected ..." in claim 9 is not understood. It is not clear whether the limitation intends to point out the switch's capability of "routing" data, whether the limitation suggests that the switch is responsible for some encryption function, or whether some other meaning of the claim is intended.

11. The term: "key material" in claims 74 and 82 is not understood. For purposes of further examination the phrase is treated as the data that <u>could</u> be used in creation of a key.

12. The phrase: "the receiver decrypts the encrypted data <u>in response to</u> the receiver key" is not understood. For purposes of further examination the phrase is treated as "the receiver key is used to decrypt the encrypted data".

13. "AE S-128 CTR protocol" is not understood.

14. Claims 4-8, 10, 12-13, 15, 17-20, 22-26, 32-35, 54-56, 75-76, 83-86 are rejected by virtue of their dependence.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

15. Claims 70-76 and 78-85 are rejected under 35 U.S.C. 102(b) as being anticipated by *Menezes et al. (Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied cryptography", 1997, ISBN: 0849385237).*

16. As per claims 70-76 and 78-85 *Menezes et al.* teach a unilateral authentication using random numbers *(Menezes et al., pg. 401, "10.16 Remark" section)* that reads on "a communication system including a transmitter; a receiver; and a communication channel between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol that includes a procedure for supplying a receiver key to the receiver, and a challenge response procedure for verifying whether the transmitter has a transmitter key matching the receiver key, wherein the receiver is configured to encrypt first data in accordance with the protocol using the receiver key to generate an authentication message, and to send the authentication message to the transmitter over the channel, the transmitter is configured to perform a predetermined mathematical function on the

authentication message to generate a result, to encrypt the result using the transmitter key to generate an encrypted result, and to send the encrypted result to the receiver over the channel, and the receiver is configured to generate a decrypted result by decrypting the encrypted result using the receiver key, and to determine whether the decrypted result satisfies a predetermined criterion".

17. *Menezes et al.* teach a receiver generating the authentication message that comprise an encrypted pseudo random value r(B) and additional data *(B*)*. *Menezes et al.* call the disclosed authentication "challenge-response by symmetric-key technique" *(Menezes et al., pg. 400)* and in the symmetric-key cryptography encrypting data with an (invalid) encryption key that does not match a decryption key will not allow (the receiver) to decrypt the data.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

18. Claims 77 and 86-87 are rejected under 35 U.S.C. 103(a) as unpatentable over *Menezes et al. (Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied cryptography", 1997, ISBN: 0849385237)* in view of *Pfleeger*

(Charles P. Pfleeger, "Security in computing", 2nd edition, 1996, ISBN: 0133374866).

19. *Menezes et al.* teach challenge-response authentication as discussed above.

20. While discussing the challenge response *Menezes et al.* do not teach an external agent coupled to the receiver and the transmitter, wherein the external agent is configured to provide an encrypted version of the receiver key.

21. *Pfleeger* discloses a communication system discussed by disclosing a key distribution protocol. In particular *Pfleeger* introduces an external agent *(a central key distribution service)* configured to be coupled to the receiver *(Renee)* and to the sender *(Pable)*, wherein at least one of the receiver and the transmitter is configured to send a ticket request to the external agent when coupled to the external agent, and the external agent is configured to respond to the request by determining or obtaining a determination as to whether to grant the request, and sending at least one signal to one of the transmitter and the receiver in response to each granted request, wherein the at least one signal is indicative of data that determines a pre-encrypted version of the key and data enabling the receiver to decrypt the pre-encrypted version of the key *(K[pr]). Pfleeger, Symmetric Key Exchange with Server, pg. 131-132).*

22. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the external agent in transmitter and receiver to distribute encryption keys as taught by *Pfleeger* given the benefit of flexible key distribution.

23. Claims 1-5, 8-26, 31-36 and 53-57 are rejected under 35 U.S.C. 103(a) as unpatentable over *Pfleeger (Charles P. Pfleeger, "Security in computing", 2nd edition, 1996, ISBN: 0133374866).*

24. As per claims 1, 12, 16, 21, 31, 36, 53 and 57 *Pfleeger* teaches a communication system including: a transmitter; a receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol; a link coupled between the transmitter and the receiver, wherein the transmitter is operable in an encryption mode in which it generates encrypted data and transmits the encrypted data over the link to the receiver, and the receiver is operable in a decryption mode in which it generates decrypted data by decrypting the encrypted data using a key *(Fig. 3-10, pg. 101).*

25. *Pfleeger* discloses an improvement to the communication system discussed by disclosing a key distribution protocol. In particular *Pfleeger* introduces an external agent *(a central key distribution service)* configured to be coupled to the receiver *(Renee)* and to the transmitter *(Pable)*, wherein at least one of the receiver and the transmitter is configured to send a ticket request to the external agent when coupled to the external agent, and the external agent is configured to respond to the request by determining or obtaining a determination as to whether to grant the request, and sending at least one signal to one of the transmitter and the receiver in response to each granted request, wherein the at least one signal is indicative of data that determines a pre-encrypted version of the key and data enabling the receiver to

decrypt the pre-encrypted version of the key *(K[pr]). Pfleeger, Symmetric Key Exchange with Server, pg. 131-132)*.

26. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the external agent in a transmitter and receiver encrypted data exchange given the benefit of flexible key distribution.

27. *Pfleeger* discloses a more common implementation of a repeater and a receiver connected through serial links and repeaters *(pg. 386-37, Inter-Networks section).*

28. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use serial links and a repeater to connect a transmitter and a receiver given the benefit of an ability to connect two distant parties exchanging data while providing increased reliability *(Advantage of Computing Networks section, pg. 389)*.

29. As discussed above it would have been obvious to utilize repeaters in order to connect two remote communicating parties. However, expanding on the advantages of connecting remote entities *Pfleeger* stresses the need to consider additional security measures, especially since in connecting remote transmitters and receivers additional intermediates are present *(Advantages of Computing Networks, pg. 389)*. As a solution to some of the security threats *Pfleeger* offers a link encryption involving a transmitter, a repeater and a receiver, wherein the transmitter and the repeater are configured to implement a content protection protocol, and the repeater and the receiver are configured to implement a second content protection protocol; a first link between the transmitter and the repeater, and second link between the repeater and the receiver, wherein the transmitter is configured to generate

encrypted data by encrypting first data using a secret value and transmit the encrypted data over the first link to the repeater, the repeater is configured to generate decrypted data including by decrypting the encrypted data using the secret value, to generate re-encrypted data including by encrypting the decrypted data using a second secret value, and to transmit the re-encrypted data over the second link, and the receiver is configured to generate additional decrypted data by decrypting the re-encrypted data using the second secret value *(Link Encryption section, pg. 406)*.

30. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement a link encryption. One of ordinary skill in the art would have been motivated to perform such a modification in order to provide communication security to address transmission line vulnerability.

31. Implementation of link encryption would essentially result in essentially the repeater forwarding encrypted data received from the at least one serial link, and generating by the receiver encrypted data by decrypting the encrypted data using a secret value in accordance with a first content protection protocol.

32. *Pfleeger* does not explicitly teach enabling the repeater and the receiver to operate in an extending utilization of the external agent to enable the repeater and the receiver to implement a content connection protocol with use of an external agent as discussed previously. However, providing the choice of engaging the external agent in the repeater and the receiver would have been obvious at least to accommodate

the need for the flexible key distribution for the communicating parties such as the repeater and the receiver.

33. Establishing a secure data exchange between a repeater and a receiver involving an external agent as disclosed by *Pfleeger* on page 131-132 would result in generating encrypted data by the repeater by performing a translation operation on multiply encrypted data received from the at least one serial link, wherein the translation operation would include decryption of the multiply encrypted data using a second secret value in accordance with a second content protection, forwarding by the repeater the encrypted data to the at least one additional serial link, and generating by the receiver decrypted data by decrypting the encrypted data in accordance with the second content protection protocol using a third secret value.

34. As per claims 12 and 16 Pfleeger teach challenge-response system in which two entities exchange data allowing "dynamic" authentication where arithmetic calculation of encryption/decryption is performed on some data *(Pfleeger, pg. 262 "One-time Password")*.

35. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include challenge-response in communication between two parties (e.g. transmitter/receiver). One of ordinary skill in the art would have been motivated to perform such a modification in order to provide a very secure authentication of communication entities such as a transmitter and a receiver.

36. Introducing a challenge-response system into the system as discussed above would result in multiply encrypted data that flows between the transmitter, the router/repeater and the receiver.

37. Also, the examiner points out that although it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement functionality in communication system as discussed above it is well-known practice to support a variety of systems in the computing arts. As a result it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to configure the transmitter, the router, the receiver and the external agent to operate in multiple modes including the mode discussed above as well as modes wherein no encryption/decryption is present. One of ordinary skill in the art would have been motivated to perform such a modification in order to allow for flexible infrastructure accommodating equipment with various capabilities.

38. As per claim 9 Official Notice is taken that it is old and well-known to use switches in a network environment and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate a switch given the benefit of fast data transmission.

39. As per claim 13 in symmetric encryption two encryption keys must be the same in order to successfully decrypt received encrypted data.

40. As per claims 10 and 35 *Pfleeger* teaches a digital signature *(pg. 140-141).*

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate in the communication system as discussed above a digital signature. One of ordinary skill in the art would have been motivated to perform such a modification in order to provide non repudiation, and sent data authenticity.

41. Claims 6-7 and 27-30 are rejected under 35 U.S.C. 103(a) as unpatentable over *Pfleeger (Charles P. Pfleeger, "Security in computing", 2nd edition, 1996, ISBN: 0133374866)* in view of *Graunke (U.S. Pub. No. 20030005285).*

42. *Pfleeger* teaches the communication system as discussed above.

43. *Pfleeger* does not teach AES protocol or HDCP protocol.

44. *Graunke* teaches AES and HDCP protocol *[6 and 24].*

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use AES and HDCP protocols as taught by *Graunke*. One of ordinary skill in the art would have been motivated to perform such a modification given benefit of a proven common block cipher as well as extended data protection of content such as music by preventing unauthorized reproduction of the content.

45. AES 128 is one of the types of AES protocol and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use such a protocol in order to encrypt/decrypt data.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

1/9/06

NORMAN M. WRIGHT
PRIMARY EXAMINER